

REMARKS/ARGUMENTS

The following Request for Reconsideration is submitted in response to the Office Action issued on June 5, 2003 (Paper No. 7) in connection with the above-identified patent application, and is being filed within the first month after the three-month shortened statutory period set for a response by the Final Office Action.

Claims 1-46 are pending in the present application, and stand rejected. Applicants respectfully request reconsideration and withdrawal of the rejection of the claims, consistent with the following remarks.

The Examiner has rejected claims 1-46 under 35 USC § 103(a) as being obvious over Matsuzaki et al. (U.S. Patent No. 6,058,476) in view of Patel (U.S. Patent No. (6,374,355)). Applicants respectfully traverse the § 103(a) rejection of such claims.

As was previously submitted, Independent claim 1 recites a method for releasing digital content to a rendering application, where the rendering application forwards the digital content to an ultimate destination by way of a path therebetween. Significantly, *the path is defined by at least one module and the digital content is initially in an encrypted form.*

In the method, an authentication of at least a portion of the path is performed to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough. If in fact each such defining module is to be trusted *based on the authentication*, the encrypted digital content is *decrypted* and forwarded to the rendering application for further forwarding to the ultimate destination by way of the authenticated path.

Independent claim 24 recites substantially the same subject matter as claim 1, albeit as a computer-readable medium having computer-executable instructions thereon that perform the method.

With the present invention, then, encrypted content is decrypted and released to a rendering application only after an authentication determines that trust may be imparted to the path that the rendering application will employ to forward the decrypted content to the ultimate destination. To summarize, then, the present invention requires (1) an authentication of a path defined by at least one module and then (2) a decryption and forwarding of content through the path, but only if the authentication succeeds. For example, in the case of an application that will forward decrypted and rendered content to an ultimate destination by way of a path defined by a plurality of content filters, the application will only be allowed to have such decrypted content *after* it is determined that the filters defining the path can be trusted to handle the decrypted content in a trusted manner. Such trust is for example with regard to the fact that the filters defining the path will not copy the decrypted content for nefarious purposes.

Thus, the present invention is especially useful when the encrypted content is of a type that should not be copied in a decrypted form, such as for example audio content in the form of a musical selection, or video content such as a commercially available movie. As may be appreciated, in the course of being authenticated, a particular module may prove its trustworthiness by, for example, proffering a digital certificate issued by an entity that may itself be deemed to be trustworthy.

The present invention as recited in the claims also requires that the path be not merely a conduit between a source and a destination, such as for example a wire or an over-

air channel, but that such path be defined by modules through which the content is to pass, such as the aforementioned filters. Thus, the present invention is especially concerned with theft by way of the module(s) defining the path, and not with theft of the content as such content is physically passed from module to module within the path. Once again, as recited in the claims, the authentication is performed with regard to at least a portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough. Thus, the present invention can be employed to restrict the content to a particular path or a particular set of modules within a path.

Once again, the Matsuzaki reference discloses a method of encrypting content for transmission between a first and a second device, where the first device encrypts the content and then transmits same to the second device in the encrypted form for decryption thereby. Accordingly, the Matsuzaki reference does not disclose or suggest decrypting the encrypted digital content and forwarding such decrypted content to a rendering application (the first device, according to the Examiner), for further forwarding to an ultimate destination (the second device, according to the Examiner) by a path, as is required by claims 1 and 24. More particularly, rather than transmitting *decrypted* content on a trusted path between the first and second devices, as is required by claims 1 and 24, the Matsuzaki reference discloses that the path need not be trusted because the content is *encrypted* while traversing such path. To summarize, then, whereas claims 1 and 24 require both authenticating a *path* and sending *decrypted* content over the authenticated path, Matsuzaki discloses only authenticating a *destination or source* and sending / receiving *encrypted* content to / from the authenticated destination or source.

Once again, the Examiner points to a cable 116 as defining the path and a SCSI controller 121 as defining a module in the path. However, and significantly, neither such SCSI controller 121 nor any other module of such path between the first device and the second device in the Matsuzaki reference is authenticated to determine whether such module is to be trusted to appropriately handle any such decrypted digital content passing therethrough, as is required by claims 1 and 24. In fact, in making the rejection, the Examiner admits that Matsuzaki fails to disclose or suggest authenticating any portion of the Matsuzaki path.

Nevertheless, the Examiner continues by arguing that the Patel reference discloses authenticating at least a portion of a path. Such Patel reference discloses in connection with a wireless communications system that a mobile unit and a base network mutually establish secure over-air communications therebetween by way of exchanging data and then mutually deriving a cryptographic key based on such exchanged data. Such key is then employed to establish encrypted communications channels by which the mobile unit and the base network communicate.

Thus, and as with the Matsuzaki reference, the Patel reference does not disclose or suggest decrypting encrypted digital content and forwarding such decrypted content through a path, as is required by claims 1 and 24. As with the Matsuzaki reference, the Patel reference discloses that the path need not be trusted because the content is *encrypted* while traversing such path. Thus, and again, whereas claims 1 and 24 require both authenticating a *path* and sending *decrypted* content over the authenticated path, both Patel and Matsuzaki disclose only authenticating a *destination or source* and sending / receiving *encrypted* content to / from the authenticated destination or source.

Moreover, the Patel reference does not even disclose or suggest that the Patel path is defined by modules through which the Patel data passes, as is the case with claims 1 and 24. Instead, in the Patel reference, the path is merely one or more ethereal over-air communications channels.

Quite simply, both the Matsuzaki and Patel references teach only that first and second devices authenticate each other, and not the path therebetween. Moreover, such references would not teach that either of such first and second devices authenticates a path therebetween for the reason that the Matsuzaki or Patel content traversing such path is encrypted. Thus, the Matsuzaki and Patel paths need not be authenticated for the reason that such paths need not be trusted.

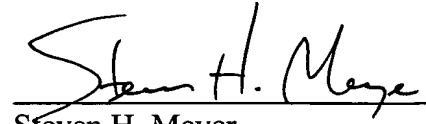
Thus, Applicants respectfully submit that neither the Matsuzaki reference nor the Patel references disclose (1) an authentication of a path defined by at least one module and (2) a decryption and forwarding of content through the path, but only if the authentication succeeds, as is required by claims 1 and 24. Accordingly, and for all the aforementioned reasons, Applicants respectfully submit that the Matsuzaki reference and the Patel reference cannot be combined to make obvious claims 1 or 24, or any claims depending therefrom, including claims 2-23 and 25-46. Thus, Applicants respectfully request reconsideration and withdrawal of the § 103(a) rejection.

In view of the foregoing discussion, Applicants respectfully submit that the present application, including claims 1-46, is in condition for allowance, and such action is respectfully requested.

DOCKET NO.: MSFT-0135/147325.1
Application No.: 09/525,510
Office Action Dated: June 5, 2003

PATENT

Date: September 17, 2003


Steven H. Meyer
Registration No. 37,189

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439